

# Defender Economics

---

Andreas Lindh, @addelindh, Troopers 15



# Who is this guy?

- From Gothenburg, Sweden
- Security Analyst at I Secure Sweden
- Used to work for a big automotive company
- Computer security philosopher
  - @addelindh -> Twitter
- Security Swiss Army knife
  - Not sharp, just versatile 😊



# What's it about?

- Understanding attackers, their capabilities and constraints
- How this information can be used to make better defensive decisions
- Bonus: provide input on how offense can get better at emulating real threats

# Inspiration

- This talk shamelessly builds on the work of some very smart people, so thanks:
  - Dan Guido (@dguido)
  - Dino Dai Zovi (@dinodaizovi)
  - Jarno Niemelä (@jarnomn)
- You should really go Twitter-stalk these guys if you aren't already

# Disclaimer



O foolish anxiety of wretched man, how  
inconclusive are the arguments which make thee  
beat thy wings below!

(Dante Alighieri)

[izquotes.com](http://izquotes.com)

# The thing about security



# Security truism #1

*“An attacker only needs to find one weakness while the defender needs to find every one.”*

*The defenders dilemma*




## Security truism #2

*“A skilled and motivated attacker will always find a way.”*



# The sky is falling

## How Malware Bypasses Our Most Advanced Security Measures



**JUNIPER**  
NETWORKS

**THE ADVANCED  
ATTACKER IS NOT AFRAID  
OF YOUR SECURITY**

Kevin Kennedy  
SENIOR DIRECTOR, PRODUCT MANAGEMENT  
COUNTER SECURITY  
JUNIPER NETWORKS



Right now, your network is unprotected.

Download the [eBook now](#)

Advanced malware infections such as "Cryptolocker" often sounds like something that happens to others. But if you're still trying to defend today's advanced threats with yesterday's signature-based security technology, your network could be next.

Begin your plan to combat, advanced threats with our eBook – a 5-point battle plan for small and midsize businesses.

Start your battle plan Now. Download the [eBook](#) today.

**IF YOU'RE NOT PROTECTED WITH FIREEYE  
YOU'RE NOT PROTECTED**

**FireEye**

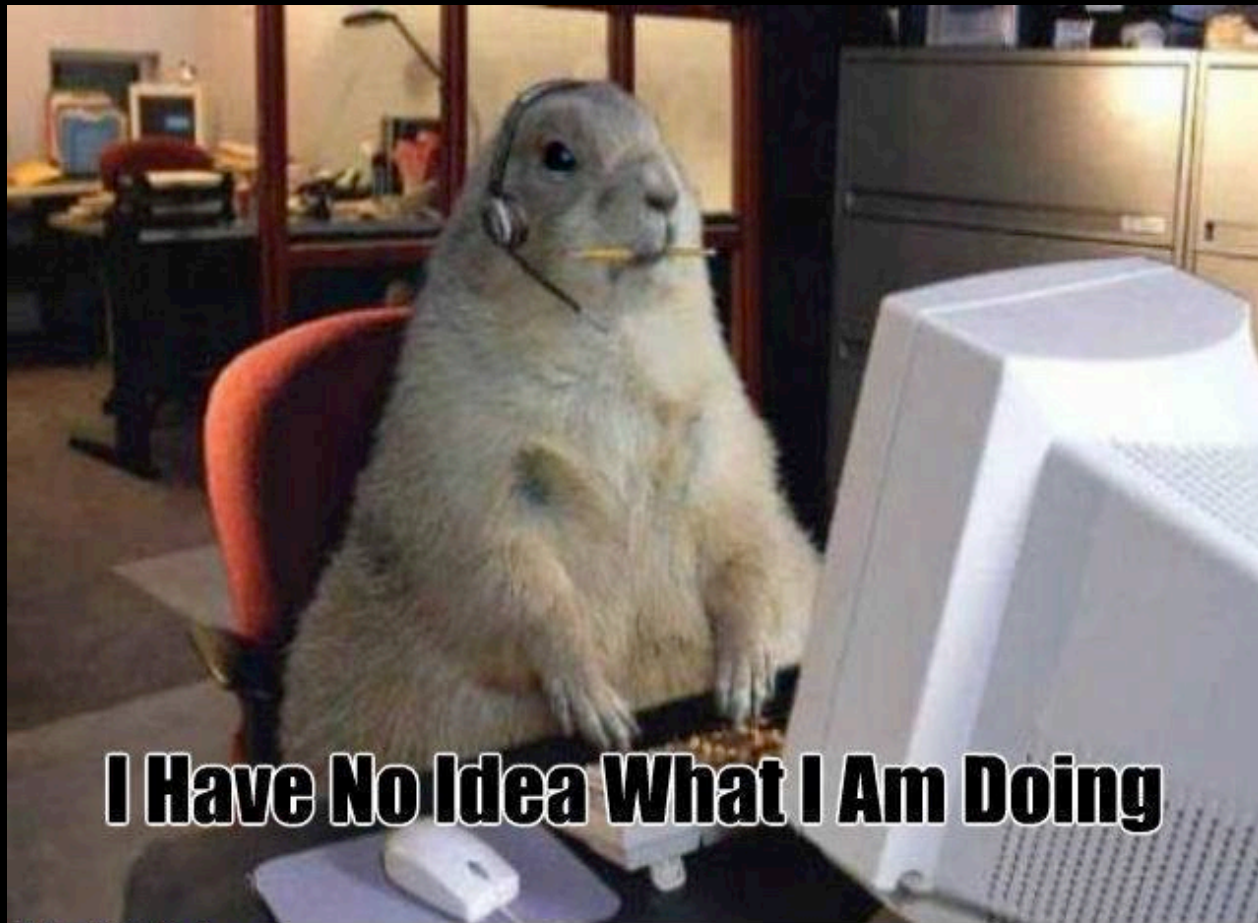
## Nation-State Cyber Espionage, Targeted Attacks Becoming Global Norm

# Attacker mythology



*Photoshop magic by Mirko Zorz @ <http://www.net-security.org>*

# Meanwhile in the CISO's office



**I Have No Idea What I Am Doing**

# The thing about the thing

- On the one hand
  - Yes, attackers are evolving
  - No, you can't protect against everything
- On the other hand
  - No attacker has infinite resources
  - Do you really *need* to protect against everything?



# Hackers vs Attackers



# Attacker considerations



# Attacker math

*“If the cost of attack is less than the value of your information to the attacker, you will be attacked.”*

*Dino Dai Zovi, “Attacker Math”\*, 2011*

*\*[https://www.trailofbits.com/resources/attacker\\_math\\_101\\_slides.pdf](https://www.trailofbits.com/resources/attacker_math_101_slides.pdf)*



# Attacker economics

- An attack has to make “economic” sense to be motivated
- An attack that is motivated has to be executed using available resources
- Bottom line: keep it within budget

# Defender economics

- Figure out your attacker's limitations
- Raise the cost of attack where your attacker is weak and you are strong
- Bottom line: break the attacker's budget

# Know your enemy



# Attacker profiling

- Motivation
- Resources
- Procedures



# Motivation

- Motivation behind the attack
- Level of motivation per target



OMG! ← Motivation-O-Meter → Meh.

# Resources

- People and skills
  - Tools and infrastructure
  - Supply chain
  - And so on...
- 
- Willingness to spend resources depends on motivation

# Procedures

- Attack vectors
  - Post-exploitation activities
  - Flexibility
  - And so on...
- 
- Procedures often designed for efficiency, reusability, and scalability



# Two very different examples



Google Chrome  
vs  
Malware



Big company X  
vs  
APT groups

# Google Chrome

- 61.6% market share  
(December 2014)
  - Source: w3schools
- 220 RCE vulnerabilities in  
2012-2014
  - Source: OSVDB
- Should be an attractive  
infection vector for malware



# Attacker profile: Malware

- Volume driven
- Drive-by downloads
- Requires file system access
- Supply chain dependency
  - Exploit Kits



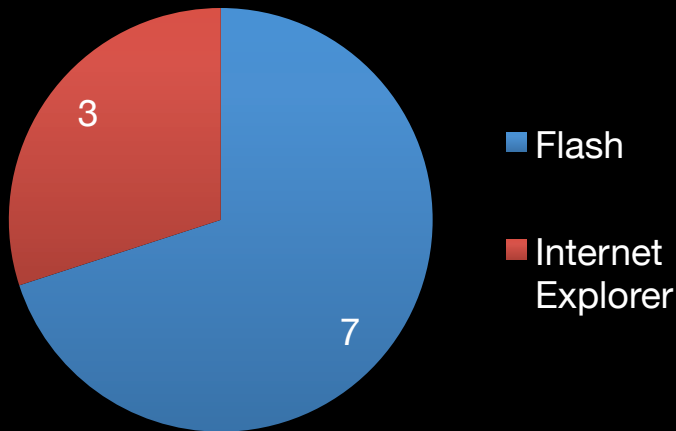
# Exploit Kits

- Most exploits not developed in-house
  - Repurposed from other sources
  - See Dan Guido's **Exploit Intelligence Project**\*
- Exploits developed for default setup
- Very few 0days
- Limited targets

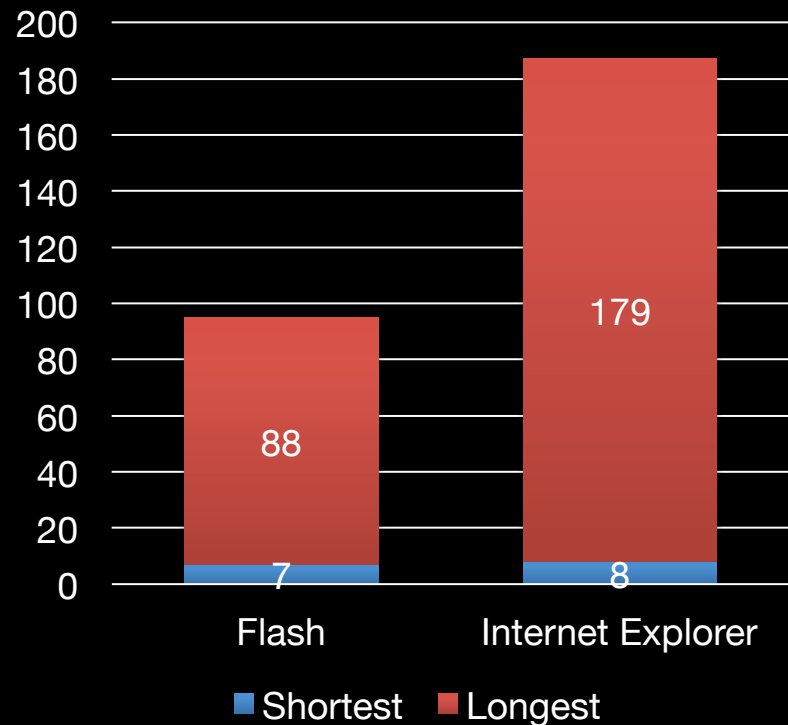
*\*[https://www.trailofbits.com/resources/exploit\\_intelligence\\_project\\_paper.pdf](https://www.trailofbits.com/resources/exploit_intelligence_project_paper.pdf)*

# 21 Exploit Kits in 2014

Exploits added in 2014



Patch-to-exploit



Source: Contagio Exploit Kit table - <http://contagiodata.blogspot.com/2014/12/exploit-kits-2014.html>

# Chrome security model

- Strong security architecture
  - Tabs, plugins run as unprivileged processes
- Rapid patch development
  - Capable of 24 hour turnaround
- Rapid patch delivery
  - Silent security updates
  - 90% of user-base patched in ~1 week

# Chrome vs Malware

- Raised cost for exploit developers
  - Usually requires multiple chained vulnerabilities for file system access
- Raised cost for Exploit Kits
  - Few publicly available exploits
  - No market for exploits that are only effective for a couple of days



# Big company X

- 50 000 employees
- Centrally managed IT
- No rapid patching
- Low security awareness among employees
- Has an APT\* problem



*\*OMG CYBER!*

# Attacker profile: APT groups

- Target driven
- Phishing
- 0ldays and 0days
- Off-the-shelf and custom tools/malware
- Post-intrusion activity
- Stealthy presence
- Professional

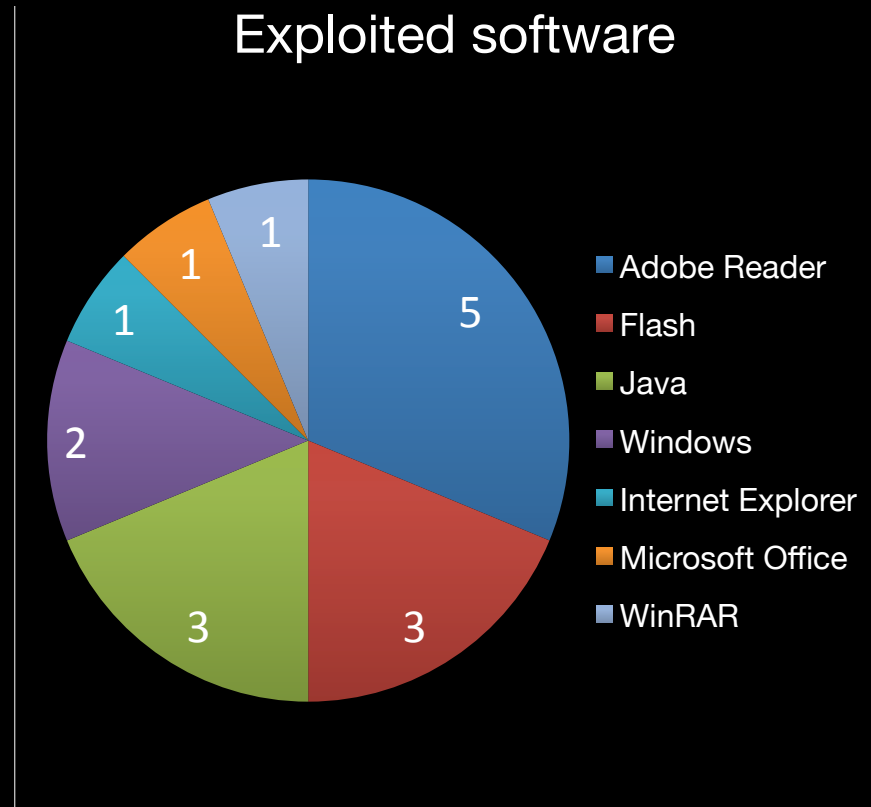
# APT groups – previous research

- “Statistically effective protection against APT attacks”\* by @jarnomn
- ~930 samples of exploits used in the wild by APT groups 2010-2013
- EMET was found to block 100% of exploits
  - Indicative but not conclusive

*\*[https://www.virusbtn.com/pdf/conference\\_slides/2013/Niemela-VB2013.pdf](https://www.virusbtn.com/pdf/conference_slides/2013/Niemela-VB2013.pdf)*

# APT groups active in 2014\*

- 13 groups
- Active from 2003
- 100% spear phishing
- ~50% has used 0days ( $\geq 2$ )
- Only one exploit bypassed “non-default”



\*Source: <https://apt.securelist.com>

# APT strengths | weaknesses

- Strengths

- Post-intrusion activity
- Stealthy presence
- Professional

- Weaknesses

- Predictable attack vector
- Unsophisticated initial intrusion



# Options for Company X

- Cheap but effective
  - Exploit mitigation
  - Secure software configurations
- More expensive and effective
  - 3<sup>rd</sup> party sandbox
- Very expensive and possibly(?) effective
  - Email security product

# Conclusion







# MASTER SPLINTER

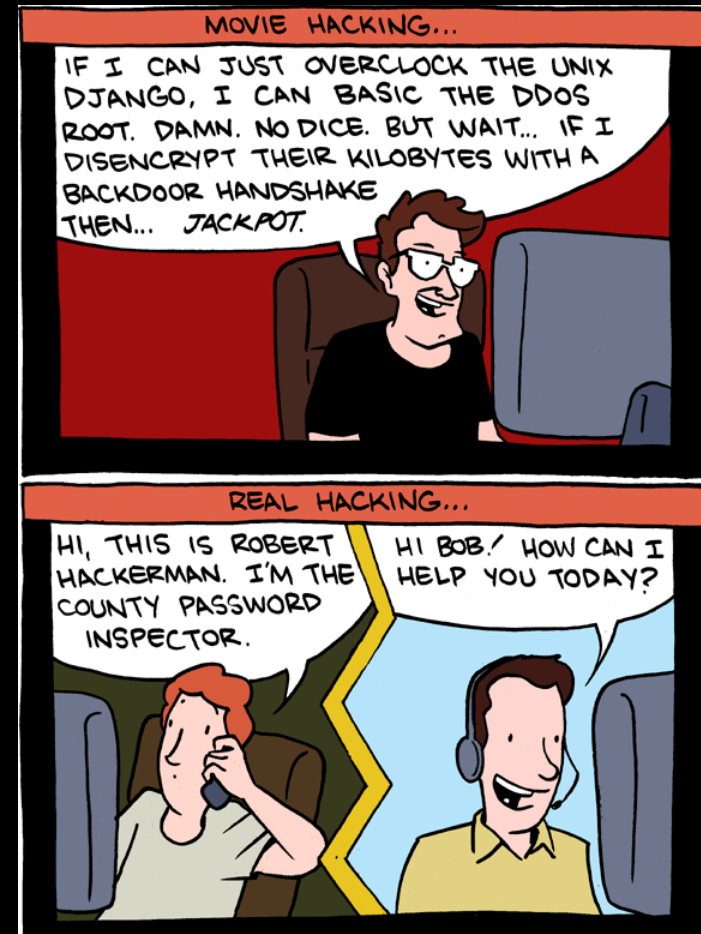
*"You do not fight the armor. You fight the man inside."*

# Security is hard, but...

- Attackers are not made of magic
- Every attacker has limitations
- Understanding these limitations is the key to making informed defensive decisions
- Raising the cost (bar) of attack can be very effective
- This is NOT about being 100% secure

# For the pentesters

- Thinking like a hacker is *not* the same as thinking like an attacker
- Understand that attackers have scopes and constraints too



**SO YOU'RE AN  
ATTACKER?**

**THAT DON'T IMPRESS ME  
MUCH**

[memegenerator.net](http://memegenerator.net)

# Thank you for listening!

Andreas Lindh, [andreas.lindh@isecure.se](mailto:andreas.lindh@isecure.se), [@addelindh](https://twitter.com/addelindh)

## Questions?